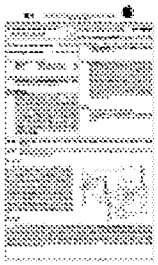
Title: **WO9966705A1: TELEPAYMENT METHOD, USING A MOBILE RADIOTELEPHONE, FOR PURCHASE OF AN ARTICLE AND/OR SERVICE**[French]

Derwent Title: Telepayment method, using a mobile phone, for purchase of an article and or service over the phone network
[Derwent Record]



High Resolution

Low Resolution

33 pages

Country: **WO** World Intellectual Property Organization (WIPO)
Kind: **A1** INTERNATIONAL APPLICATION PUBLISHED WITH INTERNATIONAL SEARCH REPORT

Inventor: **CAPITANT, Arnaud**; 1, allée de la Brède, F-45650 St. Jean-le-Blanc, France
FRANCOIS, Christophe; 63, rue Jacques Dulud, F-92200 Neuilly-sur-Seine, France
FREY, Sophie; 55, rue de Paris, F-78100 St. Germain-en-Laye, France
HITTI, Abdallah; 34, rue d'Hermemont, F-78100 St. Germain-en-Laye, France
JEAN MARIE, Olivier; 4, résidence Martin, F-78490 Bazoches, France
LUCAS, Philippe; 15, rue de l'Abbé Lambert, F-91200 Palaiseau, France
MERCIER, Philippe; 2, rue de Reims, F-75013 Paris, France
WARY, Jean-Pierre; 3 ter, rue André Theuriet, F-92340 Bourg-la-Reine, France

Assignee: **SOCIETE FRANCAISE DU RADIOTELEPHONE**, 1, place Carpeaux, F-92915 Paris la Défense, France
News, Profiles, Stocks and More about this company

Published / Filed: **1999-12-23** / 1999-06-15

Application Number: **WO1999FR0001436**

IPC Code: Advanced: B65G 61/00; G06Q 10/00; G06Q 20/00; G06Q 30/00; G06Q 40/00; H04L 29/06; H04W 12/06;
Core: H04W 12/00; more...
IPC-7: G07F 7/08; H04M 15/00;

ECLA Code: **H04L29/06S10A**; G06Q20/00K2B; G06Q20/00K4D; G06Q20/00K5; H04W12/06; T04Q7/38A; T04L29/06S8;

Priority Number: 1998-10-23 FR1998000013471

Abstract: The invention concerns a secure telepayment method, by means of a mobile telephone (1) used by the purchaser (2),

for an article and/or a service purchased by the buyer from a supplier (7). The mobile radiotelephone enables access to a radio communication network (5) managed by a management centre (6). A payment server (4) is connected to the radio communication network (5). The invention is characterised in that the method comprises a step which consists in identifying said purchaser (2) by said management centre (6) and/or by said payment server (4) and/or a control unit, the purchaser identification consisting in ensuring that the purchaser is a subscriber duly registered on the list of said radio communication network (5) subscribers. The method can further include a step which consists in authenticating said purchaser (2). [French]

Attorney, Agent or Firm: **VIDON, Patrice** ;

INPADOC Legal Status: Show legal status actions Get Now: Family Legal Status Report

Designated Country: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW, **European patent:** AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE, **OAPI patent:** BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG, **ARIPO patent:** GH GM KE LS MW SD SL SZ UG ZW, **Eurasian patent:** AM AZ BY KG KZ MD RU TJ TM

Family: Show 13 known family members

First Claim: Show all claims

REVENDICATIONS 1. Procédé pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile (1) utilisé par un acheteur (2), un bien et/ou un service acquis par ledit acheteur auprès d'un fournisseur (7), ledit radiotéléphone mobile permettant l'accès à un réseau de radi ocommuni cation (5) géré par un centre de gestion (6), un serveur de paiement (4) étant raccordé audit réseau de radi ocommuni cation (5), caractérisé en ce que ledit procédé comprend l'étape suivante :

Description Expand description

*** PROCEDE POUR PAYER A DISTANCE AU MOYEN D'UN RADIOTELEPRONE MOBILE, L'ACQUISITION D'UN BIEN ET/OU D'UN SERVICE La présente invention concerne un procédé pour payer à distance, au moyen d'un radiotéléphone mobile, l'acquisition d'un bien et/ou d'un service. L'invention concerne également un système et un radiotéléphone mobile permettant la mise en oeuvre d'un tel procédé.**

Elle s'applique à tous types de radiotéléphones mobiles, c'est-à-dire aussi bien à ceux comprenant uniquement un terminal, qu'à ceux comprenant un terminal coopérant avec un module d'identification d'abonné.

Forward References: **Go to Result Set:** Forward references (3)

PDF	Patent	Pub.Date	Inventor	Assignee	Title
	US7379920	2008-05-27	Leung; Gary		System and method for facilitating electronic financial transactions using a mobile telecommunication device
	US7047559	2006-05-16	Ohmori; Mutsuhiro	Sony Corporation	Information processing apparatus and method, recording medium, and service providing system
	US6915124	2005-07-05	Kiessling; Johan	Telefonaktiebolaget L M Ericsson (publ)	Method and apparatus for executing secure data transfer in a wireless network

Other Abstract Info: DERABS G2000-136933 DERABS G2000-136933

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 :
H04M 15/00, G07F 7/08

A1

(11) Numéro de publication internationale: **WO 99/66705**

(43) Date de publication internationale: 23 décembre 1999 (23.12.99)

(21) Numéro de la demande internationale: PCT/FR99/01436

(22) Date de dépôt international: 15 juin 1999 (15.06.99)

(30) Données relatives à la priorité:

98/07666	15 juin 1998 (15.06.98)	FR
98/13471	23 octobre 1998 (23.10.98)	FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SOCIETE FRANCAISE DU RADIOTELEPHONE [FR/FR]; 1, place Carpeaux, F–92915 Paris la Défense (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CAPITANT, Arnaud [FR/FR]; 1, allée de la Brède, F–45650 St. Jean–le–Blanc (FR). FRANCOIS, Christophe [FR/FR]; 63, rue Jacques Dulud, F–92200 Neuilly–sur–Seine (FR). FREY, Sophie [FR/FR]; 55, rue de Paris, F–78100 St. Germain–en–Laye (FR). HITTI, Abdallah [FR/FR]; 34, rue d'Hermemont, F–78100 St. Germain–en–Laye (FR). JEAN MARIE, Olivier [FR/FR]; 4, résidence Martin, F–78490 Bazoches (FR). LUCAS, Philippe [FR/FR]; 15, rue de l'Abbé Lambert, F–91200 Palaiseau (FR). MERCIER, Philippe [FR/FR]; 2, rue de Reims, F–75013 Paris (FR). WARY, Jean–Pierre [FR/FR]; 3 ter, rue André Theuriet, F–92340 Bourg–la–Reine (FR).

(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F–35700 Rennes (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

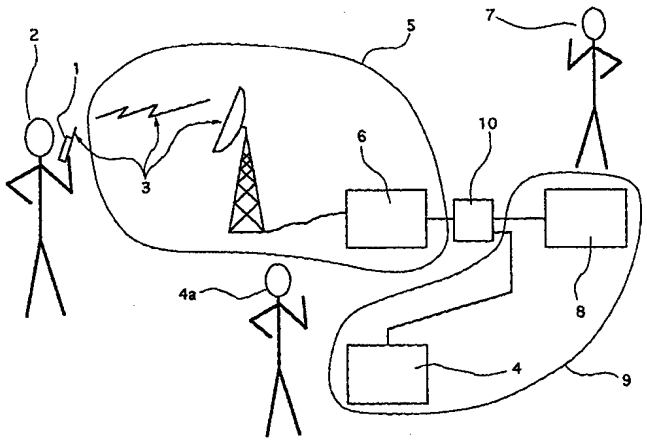
Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: TELEPAYMENT METHOD, USING A MOBILE RADIOTELEPHONE, FOR PURCHASE OF AN ARTICLE AND/OR SERVICE

(54) Titre: PROCEDE POUR PAYER A DISTANCE, AU MOYEN D'UN RADIOTELEPHONE MOBILE, L'ACQUISITION D'UN BIEN ET/OU D'UN SERVICE

(57) Abstract

The invention concerns a secure telepayment method, by means of a mobile telephone (1) used by the purchaser (2), for an article and/or a service purchased by the buyer from a supplier (7). The mobile radiotelephone enables access to a radio communication network (5) managed by a management centre (6). A payment server (4) is connected to the radio communication network (5). The invention is characterised in that the method comprises a step which consists in identifying said purchaser (2) by said management centre (6) and/or by said payment server (4) and/or a control unit, the purchaser identification consisting in ensuring that the purchaser is a subscriber duly registered on the list of said radio communication network (5) subscribers. The method can further include a step which consists in authenticating said purchaser (2).



(57) Abrégé

L'invention concerne un procédé pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile (1) utilisé par un acheteur (2), un bien et/ou un service acquis par l'acheteur auprès d'un fournisseur (7). Le radiotéléphone mobile permet l'accès à un réseau de radiocommunication (5) géré par un centre de gestion (6). Un serveur de paiement (4) est raccordé au réseau de radiocommunication (5). Selon la présente invention, le procédé comprend une étape d'identification dudit acheteur (2) par ledit centre de gestion (6) et/ou par ledit serveur de paiement (4) et/ou un centre de contrôle, l'identification de l'acheteur consistant à s'assurer que l'acheteur est un abonné régulièrement inscrit sur une liste des abonnés audit réseau de radiocommunication (5). Le procédé peut comprendre en outre une étape d'authentification dudit acheteur (2).

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE POUR PAYER A DISTANCE AU MOYEN D'UN RADIOTELEPHONE MOBILE, L'ACQUISITION D'UN BIEN ET/OU D'UN SERVICE

La présente invention concerne un procédé pour payer à distance, au moyen d'un radiotéléphone mobile, l'acquisition d'un bien et/ou d'un service. L'invention concerne également un système et un radiotéléphone mobile permettant la mise en oeuvre d'un tel procédé.

Elle s'applique à tous types de radiotéléphones mobiles, c'est-à-dire aussi bien à ceux comprenant uniquement un terminal, qu'à ceux comprenant un terminal coopérant avec un module d'identification d'abonné.

Dans le standard GSM, le radiotéléphone mobile (aussi appelé "station mobile") est du second type, et le terminal et le module d'identification d'abonné qui le composent sont appelés respectivement "équipement mobile" et "carte SIM" (pour "Subscriber Identity Module" en anglais). On rappelle qu'une carte SIM se présente sous la forme d'une carte à microprocesseur que l'on glisse dans le radiotéléphone mobile. Elle contient toutes les informations individuelles propres à l'abonné, et en particulier le numéro international d'abonné (ou IMSI, pour "International Mobile Subscriber Identity" en anglais) de ce dernier, ainsi qu'une clé d'authentification individuelle (appelée Ki) et un algorithme d'authentification individuelle (appelé A3/A8).

Divers procédés et systèmes de paiement électronique ont déjà été proposés.

Le brevet EP 451 057 B1, publié le 9 octobre 1991, décrit un procédé et un système mettant en oeuvre un serveur de paiement. La solution préconisée dans ce brevet implique l'utilisation d'une carte émettant un signal vocal d'identification. Ce signal est reçu par le microphone du téléphone puis transmis au serveur de paiement.

La demande de brevet WO 96/32701, publiée le 17 octobre 1996, décrit également un procédé de paiement électronique mettant en oeuvre un serveur de paiement. Il permet d'effectuer des transactions liées à l'achat de biens offerts par des marchands au moyen de services télématiques via un réseau de télécommunication informatique ouvert, par exemple le réseau "Internet", sur lequel sont connectés des postes serveurs de marchands et des postes clients ainsi qu'un poste serveur de paiement.

Dans le cadre de la présente invention, on suppose que le paiement de biens ou de services à distance, au moyen d'un radiotéléphone mobile, est effectué via un réseau de radiocommunication de type fermé. Par réseau de radiocommunication fermé, on entend notamment, mais non exclusivement, les réseaux basés sur la technologie GSM (par exemple le GSM 900, le DCS 1800, ...).

On rappelle qu'un réseau de radiocommunication fermé peut bien sûr être relié à un (ou plusieurs) réseau(x) ouvert(s), par l'intermédiaire de plateformes ou passerelles. Ainsi, un usager du réseau de radiocommunication fermé peut, avec son radiotéléphone mobile, accéder à un réseau ouvert. Par exemple, l'accès au réseau ouvert "Internet" est possible avec un radiotéléphone mobile, à partir d'un réseau GSM, si le radiotéléphone mobile possède des moyens (tels qu'un navigateur, ou "browser") de mise en oeuvre d'un protocole basé sur un langage spécifique, tel que le langage HDML (pour "Handset Device Markup Language" en anglais, ou "langage hypertexte pour terminaux portables") ou WML (pour "Wireless Markup Language" en anglais, ou "langage hypertexte pour terminaux sans fil"), ou encore tout autre langage du même type et/ou dérivé de l'un des deux langages précités.

Or, du fait qu'un réseau de radiocommunication fermé n'appartient pas à la catégorie des réseaux de télécommunication informatiques ouverts, la solution préconisée par la demande WO 96/32701 ne peut s'appliquer au problème posé par l'invention (à savoir le paiement de biens ou de services à distance, au moyen d'un radiotéléphone mobile).

La présente invention a précisément pour but de fournir un procédé permettant de payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile, un bien et/ou un service acquis par un acheteur auprès d'un fournisseur.

L'invention a également pour objectif de fournir un tel procédé de paiement qui minimise les interventions de l'acheteur, tout en offrant une sécurité optimale.

Ces différents objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un procédé pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile utilisé par un acheteur, un bien et/ou un service acquis par ledit acheteur auprès d'un fournisseur, ledit radiotéléphone mobile permettant l'accès à un réseau de radiocommunication géré par un centre de gestion, un serveur de paiement étant raccordé audit réseau de radiocommunication,

ledit procédé comprenant l'étape suivante :

- identification dudit acheteur par ledit centre de gestion et/ou par ledit serveur de paiement et/ou un centre de contrôle, ladite identification de l'acheteur consistant à s'assurer que l'acheteur est un abonné régulièrement inscrit sur une liste des abonnés audit réseau de radiocommunication.---

Ainsi, au terme de cette étape d'identification de l'acheteur, le gestionnaire du serveur de paiement est assuré que l'acheteur fait licitement partie du réseau de radiocommunication auquel le serveur de paiement est raccordé.

Il est à noter que dans le cas où l'identification de l'acheteur est effectuée par le centre de gestion du réseau de radiocommunication, l'opérateur de radiocommunication (qui assure le fonctionnement de ce centre de gestion) devient, dans le cadre de la présente invention, un "semi-tiers de confiance" vis-à-vis de l'organisme bancaire (qui assure le fonctionnement du serveur de paiement). En effet, dans ce cas, l'organisme bancaire se contente d'authentifier l'acheteur, l'identification du titulaire du radiotéléphone mobile étant confiée à l'opérateur.

Préférentiellement, ladite étape d'identification de l'acheteur comprend elle-même les étapes successives suivantes :

- identification d'abonné, permettant audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle de se voir communiquer un identifiant d'abonné propre audit acheteur, en tant qu'utilisateur dudit réseau de radiocommunication ;
- authentification d'abonné, permettant audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle de contrôler ledit identifiant d'abonné qui lui(leur) a été communiqué lors de ladite étape d'identification d'abonné.

Ainsi, au cours de la première étape d'identification de l'acheteur, on tire avantageusement profit du fait que, dans un réseau de radiocommunication fermé (par exemple de type GSM), l'abonné doit être identifié et authentifié par l'opérateur en charge de la tarification pour éviter la fraude et veiller à ce que la facturation soit correcte. De façon astucieuse, on utilise donc la sécurisation sur des couches physiques qu'offre un réseau fermé, par exemple du type GSM. On rappelle que dans un réseau

ouvert, tel que par exemple Internet, la sécurisation est au contraire réalisée au niveau applicatif.

De façon préférentielle, ladite étape d'authentification d'abonné comprend elle-même les étapes suivantes :

- fourniture d'un nombre aléatoire audit radiotéléphone mobile, par ledit centre de gestion et/ou ledit serveur de paiement et/ou ledit centre de contrôle;
- génération d'une signature électronique d'abonné par ledit radiotéléphone mobile :
  * avec un algorithme d'authentification individuelle et/ou une clé d'authentification individuelle contenus dans des zones protégées du radiotéléphone mobile, et
  * à partir dudit nombre aléatoire ;
- transmission de ladite signature électronique d'abonné audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle, par le radiotéléphone mobile ;
- contrôle de ladite signature électronique d'abonné par ledit centre de gestion et/ou ledit serveur de paiement et/ou ledit centre de contrôle.

Ainsi, on utilise lors de l'étape d'identification de l'acheteur la procédure d'authentification d'abonné prévue dans la norme GSM. Il est important de noter que procédure d'authentification d'abonné ne doit en aucun cas être confondue avec la procédure d'authentification de l'acheteur.

Préférentiellement, ledit procédé comprend en outre une étape d'authentification dudit acheteur, et éventuellement d'une décision d'achat du bien et/ou du service acquis par l'acheteur, par ledit et/ou un centre de gestion et/ou par ledit serveur de paiement et/ou par ledit centre de contrôle.

Ainsi, au terme de cette étape d'authentification de l'acheteur, le gestionnaire du serveur de paiement est assuré que l'acheteur est habilité à payer les biens et/ou les services acquis. Le gestionnaire du serveur de paiement peut donc autoriser ou faire procéder aux compensations entre le compte de l'acheteur et celui du fournisseur.

Dans un mode de réalisation préférentiel de l'invention, ladite étape d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend elle-même les étapes suivantes :

- génération d'une signature électronique d'acheteur par le radiotéléphone mobile ;
- transmission de ladite signature électronique d'acheteur audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle, par le radiotéléphone mobile ;
- contrôle de ladite signature électronique d'acheteur par ledit centre de gestion et/ou ledit serveur de paiement et/ou ledit centre de contrôle, ladite signature électronique d'acheteur étant tenue à la disposition de l'acheteur et du fournisseur.

Selon une variante avantageuse, ladite étape d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend elle-même les étapes suivantes :

- introduction dans le radiotéléphone mobile, par l'acheteur, au moyen d'un clavier associé au radiotéléphone mobile, d'un code de paiement confidentiel ;
- transmission de façon sécurisée dudit code de paiement confidentiel audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle, par le radiotéléphone mobile ;
- contrôle dudit code de paiement confidentiel par ledit centre de gestion et/ou ledit serveur de paiement et/ou ledit centre de contrôle.

Ainsi, selon cette variante, il n'est pas nécessaire de calculer une signature. Par transmission de façon sécurisée, on entend par exemple une transmission sous forme cryptée.

Avantageusement, ladite étape d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend en outre une étape d'introduction dans le radiotéléphone mobile, par l'acheteur, au moyen d'un clavier associé au radiotéléphone mobile, d'un code de paiement confidentiel ; ladite signature électronique d'acheteur étant générée notamment en fonction dudit code de paiement confidentiel.

Cette étape, optionnelle, permet d'accroître la sécurisation de l'authentification de l'acheteur.

On peut prévoir deux variantes de réalisation avantageuses de cette étape d'introduction du code de paiement confidentiel.

Dans la première variante, cette étape est effectuée à l'aide d'un algorithme de saisie stocké dans ledit radiotéléphone mobile. Ainsi, dans cette première variante, le

radiotéléphone assure le stockage permanent (dans le terminal et/ou le module d'identification d'abonné) de l'algorithme de saisie. Elle nécessite donc quelques adaptations au sein du radiotéléphone (dans le terminal et/ou le module d'identification d'abonné).

Dans la seconde variante, cette étape est effectuée à l'aide d'au moins une page téléchargée, au format HDML ou équivalent, et prévue à cet effet. Ainsi, dans cette seconde variante, le radiotéléphone n'assure aucun stockage permanent d'un quelconque algorithme de saisie.

Préférentiellement, ladite étape de génération d'une signature électronique d'acheteur est effectuée avec un algorithme de sécurisation de paiement et/ou une clé de sécurisation de paiement contenus dans des zones protégées du radiotéléphone mobile, et à partir de données relatives à la transaction et/ou de données relatives à l'acheteur.

On notera que la signature électronique d'acheteur permet d'authentifier soit uniquement l'acheteur, soit l'acheteur et la décision d'achat, selon qu'elle prend en compte ou non des données relatives à la transaction. Elle permet d'arbitrer les éventuelles contestations entre l'acheteur et/ou le fournisseur et/ou le serveur de paiement. Elle est essentielle en cas de contestation.

Avantageusement, au moins certaines desdites données relatives à la transaction incluent une variabilité.

De façon avantagseuse, ledit algorithme de sécurisation de paiement et/ou ladite clé de sécurisation de paiement est (sont) stocké(s) dans des zones protégées dudit terminal. Selon une variante avantageuse, le stockage est fait dans des zones protégées dudit module d'identification d'abonné.

De façon avantageuse, ledit procédé comprend en outre l'étape suivante : déverrouillage du radiotéléphone mobile, en cas de comparaison positive d'un code d'identification confidentiel, contenu dans des zones protégées du radiotéléphone mobile, à un code secret, connu de l'acheteur et introduit par ce dernier dans le radiotéléphone mobile au moyen d'un clavier.

Ce "déverrouillage" (parfois aussi appelé "initialisation") du radiotéléphone mobile est une vérification supplémentaire optionnelle, connue en soi, et offerte par certains opérateurs, notamment dans les réseaux de type GSM. On rappelle que le code

d'identification personnel (ou code PIN, pour "Personal Identity Number" en anglais) est saisit par l'abonné par exemple à chaque introduction du module d'identfication d'abonné dans le terminal, ou à chaque mise en service de ce dernier.

Préférentiellement, au moins certaines desdites zones protégées du radiotéléphone mobile sont comprises dans un module d'identification d'abonné.

Il est en effet préférable, pour des raisons de sécurité et afin de rendre le terminal aussi indépendant que possible de l'utilisateur, de confiner un maximum d'informations personnelles et confidentielles (algorithme et clé d'authentification individuelle, algorithme et clé de sécurisation de paiement, ...) dans le module d'identification d'abonné.

Avantageusement, ledit procédé comprend en outre l'étape suivante : cryptage des données relatives au règlement de l'acquisition du biens et/ou du service, échangées entre le radiotéléphone mobile et le centre de gestion et/ou le serveur de paiement et/ou le centre de contrôle, de façon que la confidentialité de l'acquisition soit assurée.

Avantageusement, ledit procédé comprend en outre l'étape suivante : contrôle de l'intégrité des données relatives au règlement de l'acquisition du biens et/ou du service, échangées entre le radiotéléphone mobile et le centre de gestion et/ou le serveur de paiement et/ou le centre de contrôle, de façon qu'un fraudeur n'aie pas la possibilité de modifier lesdites données.

Dans un mode de réalisation préférentiel de l'invention, ledit acheteur est associé à un portefeuille électronique comprenant :

- un identifiant de portefeuille, associé à un identifiant d'abonné propre audit acheteur en tant qu'utilisateur dudit réseau de radiocommunication ;
- des moyens de paiement ;
- des informations relatives audit acheteur et/ou au(x) compte(s) dudit acheteur;

l'utilisation desdits moyens de paiement, notamment lors d'un achat d'un bien et/ou d'un service, n'étant autorisée qu'après identification, et éventuellement authentification, réussie(s) de l'acheteur.

L'identification et l'éventuelle authentification de l'acheteur peuvent ainsi être vues comme l'identification et l'éventuelle l'authentification du portefeuille électronique de cet acheteur. On peut prévoir plusieurs cas, tels que par exemple :

- un abonné (et un module d'identification d'abonné correspondant) est associé à un unique portefeuille électronique ;
- plusieurs abonnés (et donc les différents modules d'identification d'abonné correspondants) partagent un même portefeuille électronique (cas par exemple d'une société détentrice du portefeuille) ;
- un même abonné (et un module d'identification d'abonné correspondant) est associé à plusieurs portefeuilles électroniques.

On notera que, du fait de la corrélation existant entre l'identifiant de portefeuille et l'identifiant d'abonné (l'abonné étant l'acheteur), l'identification de l'acheteur (en tant qu'abonné) fournit une identification implicite du porte-feuille électronique de celui-ci. On notera que dans le troisième cas précité, l'un des portefeuilles électroniques de l'abonné est par exemple choisi par défaut ou, selon une variante, on offre à l'acheteur la possibilité d'effectuer un choix parmi la pluralité de portefeuilles électroniques dont il dispose.

Après identification, et éventuellement authentification, l'acheteur peut effectivement utiliser les moyens de paiement compris dans son portefeuille électronique.

Avantageusement, ledit portefeuille électronique comprend en outre un code de paiement confidentiel, connu dudit acheteur. On rappelle que ce code de paiement confidentiel, saisi par l'acheteur au clavier du radiotéléphone, peut être pris en compte lors du calcul de la signature électronique d'acheteur, qui permet d'authentifier l'acheteur et éventuellement la décision d'achat.

Préférentiellement, ledit portefeuille électronique est stocké dans l'un des éléments appartenant au groupe comprenant : ledit terminal, ledit module d'identification d'abonné, ledit serveur de paiement, ledit centre de gestion et ledit centre de contrôle.

En d'autres termes, diverses localisations du portefeuille électronique peuvent être envisagées sans sortir du cadre de la présente invention.

L'invention concerne aussi un système de paiement à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile utilisé par un acheteur, un bien et/ou un service acquis par l'acheteur auprès d'un fournisseur.

L'invention concerne aussi un radiotéléphone mobile employé par un acheteur pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par l'acheteur auprès d'un fournisseur.

Ce système et ce radiotéléphone selon l'invention comprennent des moyens permettant la mise en oeuvre du procédé précité.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante de différentes variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif, et des dessins annexés, dans lesquels :

- la figure 1 présente une vue d'ensemble schématique d'un mode de réalisation particulier d'un système selon l'invention ;
- la figure 2 présente une vue, sous la forme de bloc diagramme, d'un mode de réalisation particulier d'un radiotéléphone mobile selon l'invention ;
- la figure 3 présente une vue, sous la forme de bloc diagramme, d'un mode de réalisation particulier d'un centre de gestion selon l'invention ;
- la figure 4 présente une vue, sous la forme de bloc diagramme, d'un mode de réalisation particulier d'un serveur de paiement selon l'invention ;
- la figure 5 présente, sous forme d'organigramme, les phases des opérations relatives à l'acquisition d'un bien et/ou d'un service ;
- la figure 6 présente un organigramme simplifié d'un mode de réalisation particulier du procédé selon l'invention ; et
- la figure 7 présente une vue, sous la forme de bloc diagramme, d'un mode de réalisation particulier d'un portefeuille électronique selon l'invention.

L'invention concerne donc un procédé, ainsi qu'un système et un radiotéléphone mobile correspondants, permettant à un acheteur de payer à distance, au moyen d'un radiotéléphone mobile, l'acquisition d'un bien et/ou d'un service.

Dans le mode de réalisation particulier présenté sur la figure 1, le système comprend un radiotéléphone mobile 1 permettant l'accès, via une liaison hertzienne 3, à un réseau de radiocommunication 5 (par exemple un réseau GSM) géré par un centre de gestion 6. Un serveur de paiement 4 et un serveur de vente 8 sont par ailleurs raccordés au réseau de radiocommunication 5.

Dans l'exemple présenté, le serveur de paiement 4 et le serveur de vente 8 sont connectés à un réseau de télécommunication informatique ouvert, par exemple le réseau Internet 9. Le réseau de radiocommunication 5 est interconnecté à ce réseau Internet 9, via une passerelle 10 (par exemple une "plateforme d'accès UP", commercialisée par la société Unwired Planet). Le radiotéléphone mobile est dans ce cas muni d'un navigateur (par exemple un navigateur "UP.browser" (marque déposée), commercialisé par la société Unwired Planet) lui permettant, via la passerelle, de naviguer au sein du réseau Internet, et d'accéder notamment au serveur de paiement 4 et au serveur de vente 8.

Le système permet à un acheteur 2 muni du radiotéléphone mobile 1, et qui est donc supposé ici être également un abonné inscrit auprès de l'opérateur du réseau de radiocommunication 5, de payer à distance de manière sécurisée, un bien et/ou un service qu'il a acquis auprès d'un fournisseur 7 disposant du serveur de vente à distance 8.

Dans le mode de réalisation particulier présenté sur la figure 2, le radiotéléphone mobile 1 comprend un terminal 20 coopérant avec une carte SIM 23. Il est clair cependant que la présente invention s'applique également à un radiotéléphone constitué du seul terminal (c'est-à-dire ne comprenant pas de module d'identification d'abonné).

De manière connue en soi, le terminal 20 comprend par exemple un module de gestion de communication 21 et un module de traitement de l'information 29, autour desquels sont interconnectés un clavier 24, un écran afficheur 26, un haut parleur 27, un microphone 28 et des moyens d'émission/réception radio 29a (comprenant une antenne).

Il est clair que l'invention s'applique plus généralement à tout type de radiotéléphone mobile. Ainsi, le terminal "classique" tel que décrit ci-dessus peut être remplacé par n'importe quel type de module de radiocommunication pouvant se connecter à un réseau de radiocommunication, tel que par exemple un terminal ne comprenant ni clavier ni écran, ou encore un microordinateur coopérant avec un terminal par l'intermédiaire d'une carte de type PCMCIA ("Personal Computer Memory Card International Association") ou équivalent.

Comme présenté sur l'organigramme de la figure 6, le procédé selon l'invention comprend les étapes suivantes :

- (optionnellement) déverrouillage (61) (ou "initialisation") du radiotéléphone mobile 1 ;
- identification (62) de l'acheteur, en tant qu'utilisateur du réseau de radiocommunication, par le centre de gestion 6 et/ou par le serveur de paiement 4 et/ou par un centre de contrôle indépendant (non représenté) ;
- (optionnellement) authentification (63) de l'acheteur, et éventuellement d'une décision d'achat d'un bien et/ou d'un service acquis par l'acheteur, par le centre de gestion 6 et/ou le serveur de paiement 4 et/ou par le centre de contrôle (non représenté).

L'étape (optionnelle) 61 de déverrouillage du radiotéléphone 1, connue en soi, se déroule par exemple de la façon suivante : l'acheteur 2 saisit au clavier 4 un numéro d'identité personnel (ou code PIN selon la terminologie GSM), puis le radiotéléphone 1 compare le numéro d'identité personnel saisi par l'acheteur avec celui stocké dans des zones protégées du radiotéléphone mobile 1 (typiquement, dans la carte SIM 23). Le radiotéléphone 1 est "déverrouillé" (c'est-à-dire opérationnel dans le réseau de radiocommunication) uniquement en cas de comparaison positive.

L'étape 62 d'identification de l'acheteur 2 consiste, selon la présente invention, à identifier et authentifier l'abonné qu'est l'acheteur lorsqu'il utilise le radiotéléphone. Cette étape 62 comprend donc par exemple les étapes classiques suivantes :

- identification d'abonné (62a), permettant au centre de gestion 6 de se voir communiquer un identifiant d'abonné propre à l'acheteur, en tant qu'utilisateur du réseau de radiocommunication. L'identifiant d'abonné 23a, ou IMSI selon la terminologie GSM, est typiquement stocké dans la carte SIM 23 ;
- authentification d'abonné (62b), permettant au centre de gestion de contrôler l'identifiant d'abonné qui lui a été communiqué lors de l'étape 62a d'identification d'abonné.

Il est à noter que l'étape d'identification de l'acheteur (consistant en une identfication et une authentification d'abonné) est effectuée de façon automatique, c'est-àdire ne nécessite aucune intervention de l'acheteur. Ce dernier n'est sollicité que lors de la phase suivante d'authentification de l'acheteur, lorsqu'il doit saisir son code de paiement confidentiel.

Il est également important de noter que l'étape 62b d'authentification de l'abonné ne doit en aucun cas être confondue avec l'étape 63 d'authentification de l'acheteur présentée en détail par la suite. En effet, l'authentification de l'abonné (qu'est l'acheteur) intervient uniquement dans le cadre de l'identification de l'acheteur. On comprend que cette identification de l'acheteur doit ensuite être complétée par une authentification de l'acheteur, de façon que le serveur de paiement vérifie que l'acheteur identifié est bien habilité à effectuer des achats.

A titre d'exemple uniquement, on rappelle maintenant, en relation avec la figure 5, le déroulement "classique", en GSM, de ces étapes d'identification 62a et d'authentification 62b d'abonné. Le radiotéléphone 1 envoie l'identifiant d'abonné (IMSI) 50 de l'utilisateur au centre de gestion 6. Après que l'abonné se soit ainsi identifié (62a), le centre de gestion 6 doit contrôler son identité, c'est-à-dire l'authentifier (62b). Pour cela, le centre de gestion 6 fournit un nombre aléatoire ("RAND") 51a au radiotéléphone 1. A partir de ce nombre aléatoire, et avec un algorithme ("A3/A8") 23b et une clé ("Ki") 23c d'authentification individuelle contenus dans des zones protégées du radiotéléphone mobile (typiquement la carte SIM 23), le radiotéléphone 1 calcule une signature électronique d'abonné ("SRES"). Cette signature électronique d'abonné 51b est transmise au centre de gestion 6 (et plus précisément à un module de gestion des abonnés 30), qui la contrôle par comparaison avec celle qu'il a calculé localement. Si les deux signatures électroniques d'abonné sont identiques, l'authentification de l'abonné (et dans le cadre de l'invention, l'identification de l'acheteur) est réussie (le titulaire du radiotéléphone mobile 1 fait partie de la liste des abonnés) et le centre de gestion renvoie des messages 51c et 52 en ce sens vers le radiotéléphone 1 et vers un module identification 40 compris dans le serveur de paiement. De plus, la technologie GSM permet une authentification indépendante de la communication établie en fonction de la topologie du réseau (à l'établissement, lors d'un handover, etc).

En résumé, après exécution de l'étape 62 d'identification de l'acheteur, le gestionnaire 4a du serveur de paiement 4 est assuré que le titulaire 2 du radiotéléphone mobile 1 (c'est-à-dire l'acheteur dans le cas présent) est régulièrement inscrit sur la liste des

abonnés et qu'il fait donc licitement partie du réseau de radiocommunication auquel le serveur de paiement 4 est raccordé.

L'étape 62 d'identification de l'acheteur est éventuellement suivie d'une étape 63 d'authentification de l'acheteur. Il s'agit pour le gestionnaire 4a du serveur de paiement 4 de s'assurer que l'acheteur 2 disposant du radiotéléphone mobile 1 au moment du règlement est habilité à payer les biens et/ou les services acquis. Si c'est effectivement le cas, le gestionnaire du serveur de paiement peut alors autoriser ou faire procéder aux compensations entre le compte de l'acheteur 2 et celui du fournisseur 7. Cette étape 63 d'authentification de l'acheteur peut être mise en oeuvre avant ou après que l'acheteur ait pris la décision d'achat.

Dans un mode de réalisation particulier, cette étape 63 d'authentification de l'acheteur comprend les étapes suivantes :

- (optionnellement) introduction dans le radiotéléphone mobile 1, par l'acheteur 2, au moyen du clavier 24, d'un code de paiement confidentiel. Cette étape d'introduction est par exemple effectuée à l'aide d'un algorithme de saisie stocké dans le radiotéléphone mobile (dans la carte SIM 23 ou dans le terminal 20) ou, selon une variante, à l'aide d'une ou plusieurs pages téléchargées, au format HDML ou équivalent, et prévues à cet effet ;
- génération d'une signature électronique d'acheteur par le radiotéléphone mobile :
  * avec un algorithme 23d et une clé 23e de sécurisation de paiement contenus dans des zones 23 protégées du radiotéléphone mobile (soit dans le terminal 20, soit dans la carte SIM 23) ;
  * à partir de données relatives à la transaction (telles que le contenu et/ou le prix) et/ou de données relatives à l'acheteur (telles que le code de paiement confidentiel, si celui-ci a été saisi par l'acheteur). En outre, les données relatives à la transaction peuvent inclure des éléments fournissant une variabilité sur la signature (tels que par exemple la date horaire de la transaction, un nombre aléatoire, un numéro de série de la transaction, etc);
- transmission de la signature électronique d'acheteur au serveur de paiement 4, par le radiotéléphone mobile 1 ;

- contrôle, dans un module de contrôle 42 compris dans le serveur de paiement 4, de la signature électronique d'acheteur. La signature électronique d'acheteur est tenue à la disposition de l'acheteur 2 et du fournisseur 7. Ce contrôle peut également être effectué par le centre de gestion des abonnés 6 ou par le centre de contrôle (non représenté). Dans le premier cas, le centre de gestion des abonnés 6 comprend un module d'authentification 33 des titulaires de radiotéléphone abonnés au service de paiement à distance.

Le déroulement de ce mode de réalisation particulier (donné à titre d'exemple) de l'étape d'authentification de l'acheteur est maintenant résumé, en relation avec la partie inférieure de la figure 5. L'acheteur 2 adresse une demande d'achat 53 au serveur de vente 8 du fournisseur 7. Il reçoit en retour les données relatives au prix du bien et/ou du service 54. L'acheteur prend ensuite une décision d'achat 55. Dans le même temps, les moyens de calcul (typiquement un microprocesseur) du radiotéléphone mobile calculent une signature électronique d'acheteur. Le radiotéléphone mobile 1 transmet, à l'aide des moyens 29a de transmission, la décision d'achat et la signature électronique d'acheteur d'une part (flèche référencée 55) au serveur 8 du fournisseur 7 et d'autre part (flèche référencée 56) au serveur de paiement 4. Le serveur de paiement 4 comprend un module de contrôle (ou de certification) 42 pour contrôler (pour certifier) la signature électronique d'acheteur. Ce module de contrôle 42 contrôle la signature en procédant par exemple à des calculs d'opérations identiques à celles effectuées dans le radiotéléphone mobile au moment de l'achat. Si la transaction est acceptée par le serveur de paiement 4, un message 57 "transaction acceptée" est adressé au serveur 8 du fournisseur, par un module accusé de réception 43 du serveur de paiement 4. Le serveur 8 du fournisseur adresse un message 58 de "confirmation d'achat" à l'acheteur (au radiotéléphone mobile de l'acheteur et/ou au domicile de l'acheteur). Les signatures électroniques d'acheteur sont stockées par un module de stockage 44 du serveur de paiement 4 et sont tenues à la disposition de l'acheteur et du fournisseur.

Il est clair que si contrôle (ou la certification) de la signature électronique d'acheteur est effectué par le centre de gestion des abonnés 6 ou par le centre de contrôle (non représenté), alors celui-ci (ceux-ci) comprend(nent) des modules de contrôle, d'accusé

de réception et de stockage du type de ceux 42, 43 et 44 décrits ci-dessus pour le serveur de paiement 4.

Selon une variante plus simple à mettre en oeuvre, l'étape 63 d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend elle-même les étapes suivantes :

- introduction dans le radiotéléphone mobile 1, par l'acheteur, au moyen d'un clavier 24 associé au radiotéléphone mobile, d'un code de paiement confidentiel. Cette étape d'introduction est par exemple effectuée à l'aide d'un algorithme de saisie stocké dans le radiotéléphone mobile (dans la carte SIM 23 ou dans le terminal 20) ou, selon une variante, à l'aide d'une ou plusieurs pages téléchargées, au format HDML ou équivalent, et prévues à cet effet ;
- transmission de façon sécurisée du code de paiement confidentiel au serveur de paiement 4, par le radiotéléphone mobile ;
- contrôle du code de paiement confidentiel par le serveur de paiement 4 (consistant par exemple à vérifier que ce code de paiement confidentiel appartient effectivement à une liste prédéterminée de codes de paiement valides).

Quel que soit le mode de réalisation choisi, à l'issue de l'étape 63 d'authentification de l'acheteur, le gestionnaire 4a du serveur de paiement 4 est assuré que l'acheteur 2 disposant du radiotéléphone mobile 1 au moment du règlement est habilité à payer les biens et/ou les services acquis. La signature électronique d'acheteur permet d'arbitrer les éventuelles contestations entre l'acheteur 2 et/ou le fournisseur 7 et/ou le gestionnaire 4a du serveur de paiement 4.

Selon la présente invention, le radiotéléphone 1 comprend, par exemple dans le module de gestion de communication 21, divers moyens nécessaires à la mise en oeuvre des différentes étapes du procédé tel que décrits ci-dessus (à travers plusieurs modes de réalisation et variantes). Notamment, le radiotéléphone comprend des moyens 22 nécessaires au déverrouillage du radiotéléphone, des moyens 24 nécessaires à l'identification de l'acheteur et des moyens 25 nécessaires à l'authentification de l'acheteur.

Les moyens de gestion de la communication et/ou les moyens de traitement de l'information 29 du radiotéléphone mobile 1 peuvent également comporter des moyens

291, permettant de crypter, de manière connue en soi, les données relatives au règlement de l'acquisition des biens et/ou des services, échangées entre le radiotéléphone mobile 1 et/ou le centre de gestion 6 et/ou le serveur de paiement 4 et/ou le centre de contrôle. Grâce à ces moyens de cryptage, la confidentialité de l'acquisition est assurée.

Les moyens de traitement de l'information 29 du radiotéléphone mobile 1 peuvent également comporter des moyens 292 permettant, de manière connue en soi, le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services, échangées entre le radiotéléphone mobile 1 et/ou le centre de gestion 6 et/ou le serveur de paiement 4 et/ou le centre de contrôle. Ainsi, un fraudeur n'a pas la possibilité de modifier ces données.

En outre, selon la présente invention, chaque acheteur peut être associé à un porte-feuille électronique 70. Comme présenté sur la figure 7, ce dernier 70 comprend par exemple :

- un identifiant de portefeuille 71, associé à un identifiant d'abonné (par exemple son "IMSI") propre à l'acheteur (en tant qu'utilisateur du réseau de radiocommunication) ;
- un code de paiement confidentiel 72, connu uniquement de l'acheteur 2 ;
- des moyens 73 de paiement, tels que notamment, mais non exclusivement, un porte-monnaie électronique 73a (généralement, pour les montants inférieurs à un seuil prédéterminé), un porte-cartes de paiement 73b (généralement, pour les montants supérieurs au seuil prédéterminé précité), ou encore tous autres moyens 73c de paiement mis à la disposition de l'acheteur par les organismes bancaires ;
- des informations 74 relatives à l'acheteur et/ou à son(ses) compte(s).

L'utilisation des moyens 73 de paiement, notamment lors d'un achat d'un bien et/ou d'un service, n'est autorisée qu'après identification, et éventuellement authentification, réussie(s) de l'acheteur 2.

Diverses localisations de stockage de ce portefeuille électronique peuvent être envisagées, à savoir dans le terminal 20, dans la carte SIM 23, dans le serveur de paiement 4, dans le centre de gestion 6 ou dans le centre de contrôle (non représenté).

REVENDICATIONS

1. Procédé pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile (1) utilisé par un acheteur (2), un bien et/ou un service acquis par ledit acheteur auprès d'un fournisseur (7), ledit radiotéléphone mobile permettant l'accès à un réseau de radiocommunication (5) géré par un centre de gestion (6), un serveur de paiement (4) étant raccordé audit réseau de radiocommunication (5),
caractérisé en ce que ledit procédé comprend l'étape suivante :

- identification (62) dudit acheteur (2) par ledit centre de gestion (6) et/ou par ledit serveur de paiement (4) et/ou un centre de contrôle, ladite identification de l'acheteur consistant à s'assurer que l'acheteur est un abonné régulièrement inscrit sur une liste des abonnés audit réseau de radiocommunication (5).

2. Procédé selon la revendication 1, caractérisé en ce que ladite étape (62) d'identification de l'acheteur comprend elle-même les étapes successives suivantes :

- identification d'abonné (62a), permettant audit centre de gestion (6) et/ou audit serveur de paiement (4) et/ou audit centre de contrôle de se voir communiquer un identifiant d'abonné (IMSI ; 23a ; 50) propre audit acheteur, en tant qu'utilisateur dudit réseau de radiocommunication ;
- authentification d'abonné (62b), permettant audit centre de gestion (6) et/ou audit serveur de paiement (4) et/ou audit centre de contrôle de contrôler ledit identifiant d'abonné qui lui(leur) a été communiqué lors de ladite étape (62a) d'identification d'abonné.

3. Procédé selon la revendication 2, caractérisé en ce que ladite étape (63) d'authentification d'abonné comprend elle-même les étapes suivantes :

- fourniture d'un nombre aléatoire (51a) audit radiotéléphone mobile, par ledit centre de gestion et/ou ledit serveur de paiement et/ou ledit centre de contrôle;
- génération d'une signature électronique d'abonné (51b) par ledit radiotéléphone mobile :
  * avec un algorithme d'authentification individuelle (23b) et/ou une clé d'authentification individuelle (23c) contenus dans des zones (23) protégées du radiotéléphone mobile (1), et
  * à partir dudit nombre aléatoire ;

- transmission de ladite signature électronique d'abonné audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle, par le radiotéléphone mobile ;
- contrôle de ladite signature électronique d'abonné par ledit centre de gestion et/ou ledit serveur de paiement et/ou ledit centre de contrôle.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit procédé comprend en outre l'étape suivante :

- authentification (63) dudit acheteur (2), et éventuellement d'une décision d'achat du bien et/ou du service acquis par l'acheteur (2), par ledit et/ou un centre de gestion (6) et/ou par ledit serveur de paiement (4) et/ou par ledit centre de contrôle.

5. Procédé selon la revendication 4, caractérisé en ce que ladite étape d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend elle-même les étapes suivantes :

- génération d'une signature électronique d'acheteur par le radiotéléphone mobile ;
- transmission (29a) de ladite signature électronique d'acheteur audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle, par le radiotéléphone mobile ;
- contrôle (42) de ladite signature électronique d'acheteur par ledit centre de gestion et/ou ledit serveur de paiement (4) et/ou ledit centre de contrôle, ladite signature électronique d'acheteur étant tenue (43, 44) à la disposition de l'acheteur et du fournisseur.

6. Procédé selon la revendication 4, caractérisé en ce que ladite étape d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend elle-même les étapes suivantes :

- introduction dans le radiotéléphone mobile (1), par l'acheteur, au moyen d'un clavier (24) associé au radiotéléphone mobile (1), d'un code de paiement confidentiel ;
- transmission de façon sécurisée dudit code de paiement confidentiel audit centre de gestion et/ou audit serveur de paiement et/ou audit centre de contrôle, par le radiotéléphone mobile ;

- contrôle dudit code de paiement confidentiel par ledit centre de gestion et/ou ledit serveur de paiement (4) et/ou ledit centre de contrôle.

7. Procédé selon la revendication 5, caractérisé en ce que ladite étape d'authentification de l'acheteur, et éventuellement de la décision d'achat, comprend en outre l'étape préalable suivante :

- introduction dans le radiotéléphone mobile (1), par l'acheteur, au moyen d'un clavier (24) associé au radiotéléphone mobile (1), d'un code de paiement confidentiel ;

et en ce que ladite signature électronique d'acheteur est générée notamment en fonction dudit code de paiement confidentiel.

8. Procédé selon l'une quelconque des revendications 6 et 7, caractérisé en ce que ladite étape d'introduction dudit code de paiement confidentiel est effectuée à l'aide d'un algorithme de saisie stocké dans ledit radiotéléphone mobile.

9. Procédé selon l'une quelconque des revendications 6 et 7, caractérisé en ce que ladite étape d'introduction dudit code de paiement confidentiel est effectuée à l'aide d'au moins une page téléchargée, au format HDML ou équivalent, et prévue à cet effet.

10. Procédé selon l'une quelconque des revendications 5 et 7 à 9, caractérisé en ce que ladite étape de génération d'une signature électronique d'acheteur est effectuée :

- avec un algorithme de sécurisation de paiement (23d) et/ou une clé de sécurisation de paiement (23e) contenus dans des zones (23) protégées du radiotéléphone mobile (1), et
- à partir de données relatives à la transaction et/ou de données relatives à l'acheteur.

11. Procédé selon la revendication 10, caractérisé en ce qu'au moins certaines desdites données relatives à la transaction incluent une variabilité.

12. Procédé selon l'une quelconque des revendications 10 et 11, ledit radiotéléphone mobile (1) comprenant un terminal (20) coopérant avec un module d'identification d'abonné (23), caractérisé en ce que ledit algorithme de sécurisation de paiement et/ou ladite clé de sécurisation de paiement est (sont) stocké(s) dans des zones protégées dudit terminal.

13. Procédé selon l'une quelconque des revendications 10 et 11, ledit radiotéléphone mobile (1) comprenant un terminal (20) coopérant avec un module d'identification d'abonné (23), caractérisé en ce que ledit algorithme de sécurisation de paiement (23d)

et/ou ladite clé de sécurisation de paiement (23e) est (sont) stocké(s) dans des zones protégées dudit module d'identification d'abonné.

14. Procédé selon l'une quelconque des revendications 1 à 13, caractérisé en ce qu'il comprend en outre l'étape suivante :

- déverrouillage (61) du radiotéléphone mobile (1), en cas de comparaison positive d'un code d'identification confidentiel (PIN), contenu dans des zones protégées (23) du radiotéléphone mobile (1), à un code secret, connu de l'acheteur et introduit par ce dernier dans le radiotéléphone mobile au moyen d'un clavier (24).

15. Procédé selon l'une quelconque des revendications 3, 10 et 12, ledit radiotéléphone mobile (1) comprenant un terminal (20) coopérant avec un module d'identification d'abonné (23), caractérisé en ce qu'au moins certaines desdites zones protégées du radiotéléphone mobile (1) sont comprises dans ledit module d'identification d'abonné.

16. Procédé selon l'une quelconque des revendications 1 à 15, caractérisé en ce qu'il comprend en outre l'étape suivante :

- cryptage (291) des données relatives au règlement de l'acquisition du biens et/ou du service, échangées entre le radiotéléphone mobile et le centre de gestion et/ou le serveur de paiement et/ou le centre de contrôle, de façon que la confidentialité de l'acquisition soit assurée.

17. Procédé selon l'une quelconque des revendications 1 à 16, caractérisé en ce qu'il comprend en outre l'étape suivante :

- contrôle (292) de l'intégrité des données relatives au règlement de l'acquisition du biens et/ou du service, échangées entre le radiotéléphone mobile et le centre de gestion et/ou le serveur de paiement et/ou le centre de contrôle, de façon qu'un fraudeur n'aie pas la possibilité de modifier lesdites données.

18. Procédé selon l'une quelconque des revendications 1 à 17, caractérisé en ce que ledit acheteur est associé à un portefeuille électronique (70) comprenant :

- un identifiant de portefeuille (71), associé à un identifiant d'abonné (IMSI ; 23a ; 50) propre audit acheteur en tant qu'utilisateur dudit réseau de radiocommunication ;
- des moyens de paiement (73, 73a, 73b, 73c) ;
- des informations (74) relatives audit acheteur et/ou au(x) compte(s) dudit acheteur;

l'utilisation desdits moyens de paiement (73), notamment lors d'un achat d'un bien et/ou d'un service, n'étant autorisée qu'après identification (62), et éventuellement authentification (63), réussie(s) de l'acheteur.

19. Procédé selon la revendication 18, caractérisé en ce que ledit portefeuille électronique (70) comprend en outre :

- un code de paiement confidentiel (72), connu dudit acheteur.

20. Procédé selon l'une quelconque des revendications 18 et 19, ledit radiotéléphone mobile (1) comprenant un terminal (20) coopérant avec un module d'identification d'abonné (23), caractérisé en ce que ledit portefeuille électronique (70) est stocké dans l'un des éléments appartenant au groupe comprenant :

- ledit terminal (20) ;
- ledit module d'identification d'abonné (23) ;
- ledit serveur de paiement (4) ;
- ledit centre de gestion (6) ;
- ledit centre de contrôle.

21. Système pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile (1) utilisé par un acheteur (2), un bien et/ou un service acquis par ledit acheteur auprès d'un fournisseur (7), ledit radiotéléphone mobile permettant l'accès à un réseau de radiocommunication (5) géré par un centre de gestion (6), un serveur de paiement (4) étant raccordé audit réseau de radiocommunication,
caractérisé en ce que ledit système comprend des moyens permettant la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 20.

22. Radiotéléphone mobile (1) employé par un acheteur pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par ledit acheteur (2) auprès d'un fournisseur (7), ledit radiotéléphone mobile permettant l'accès à un réseau de radiocommunication (5) géré par un centre de gestion (6), un serveur de paiement (4) étant raccordé audit réseau de radiocommunication,
caractérisé en ce que ledit radiotéléphone comprend des moyens permettant la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 20.

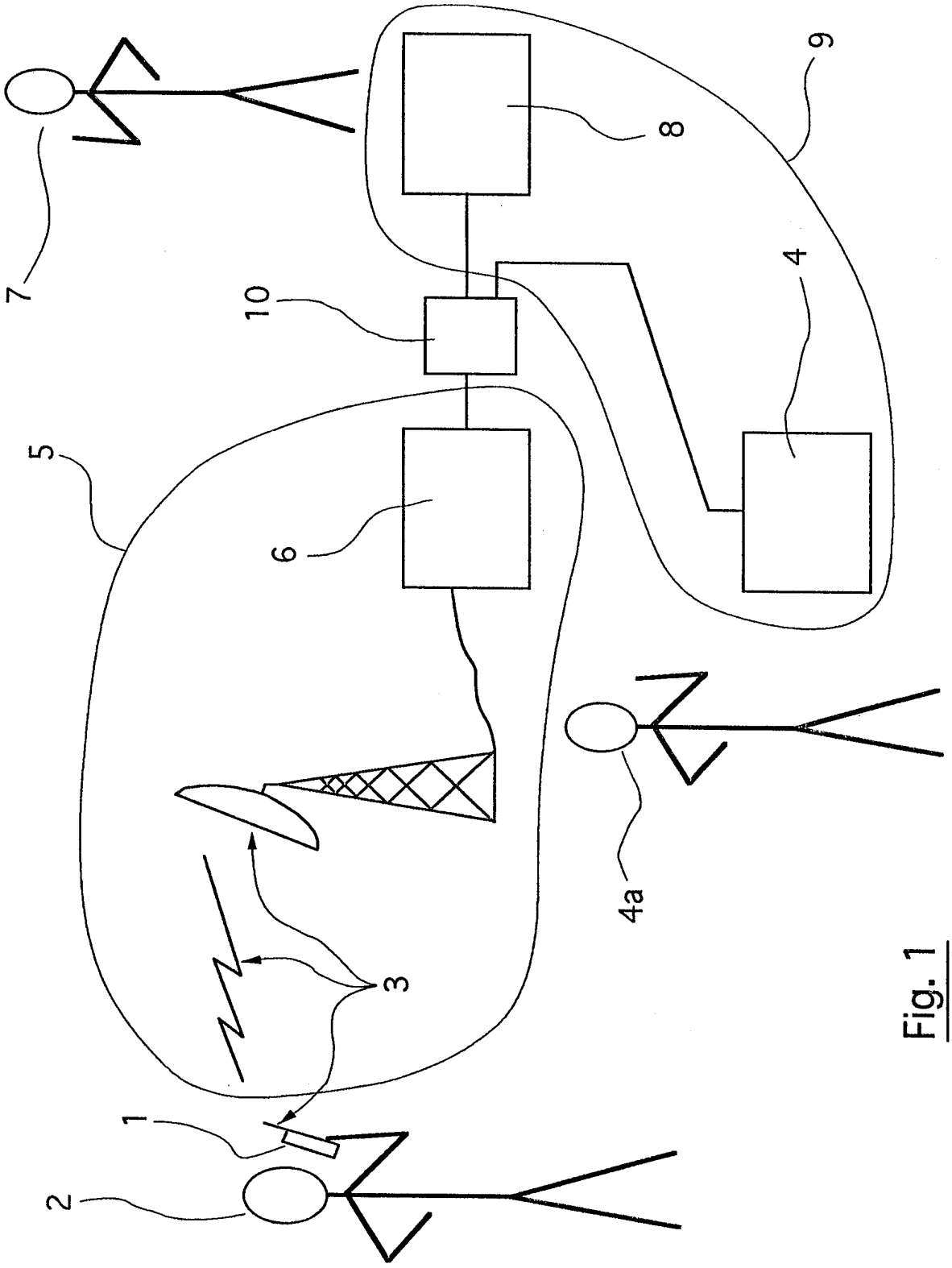


Fig. 1

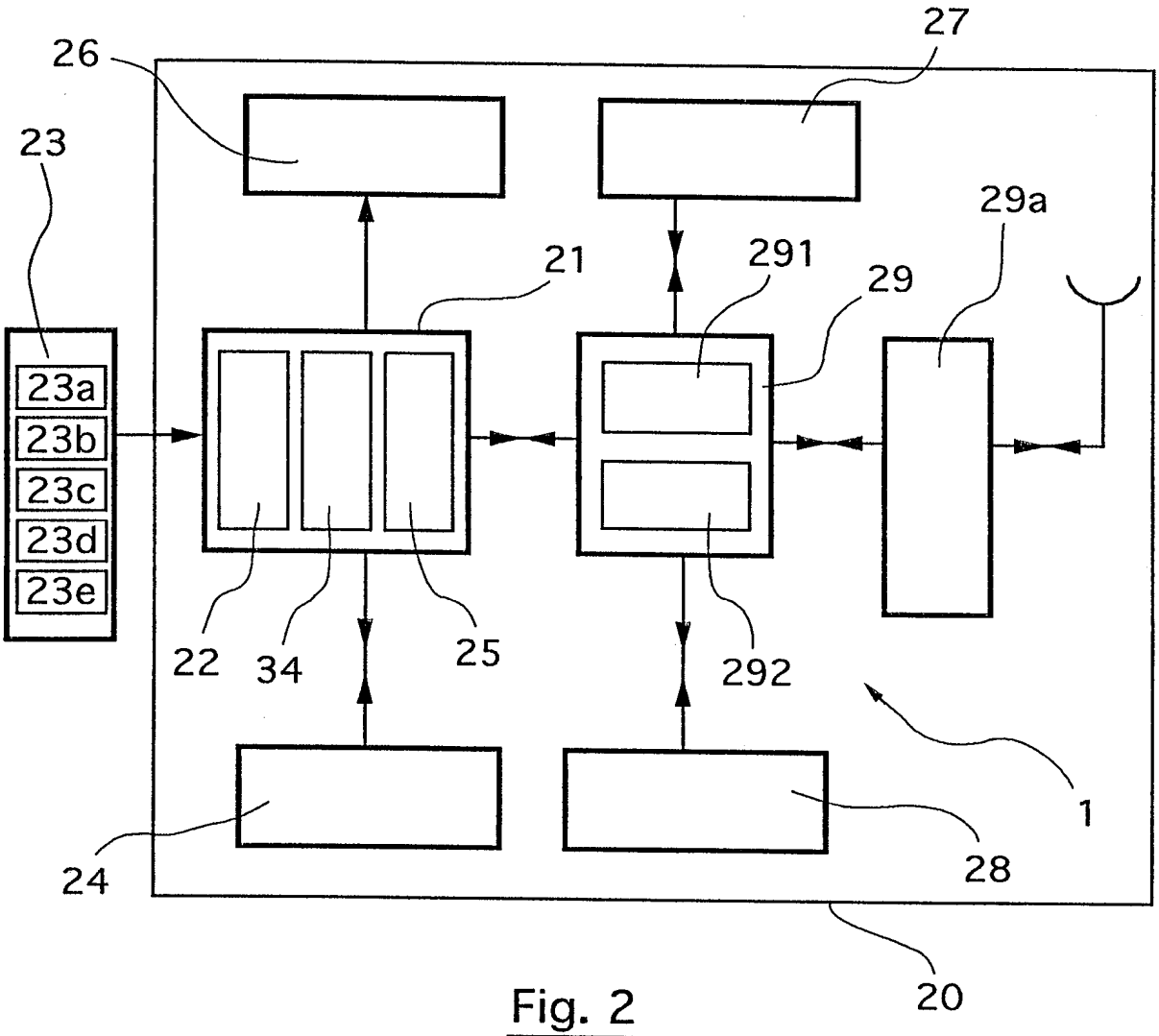

26
27
23
29a
21
291
29
23a
23b
23c
23d
23e
22
34
25
292
1
24
28
20

Fig. 2

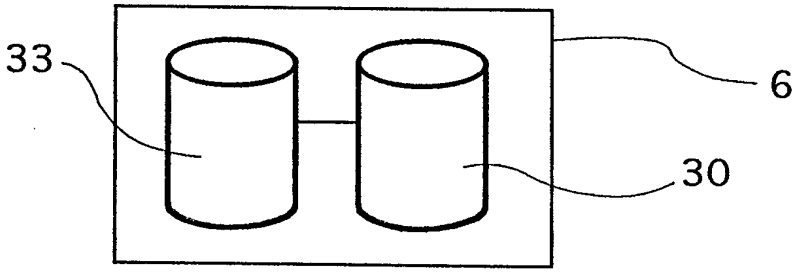

33
6
30

Fig. 3

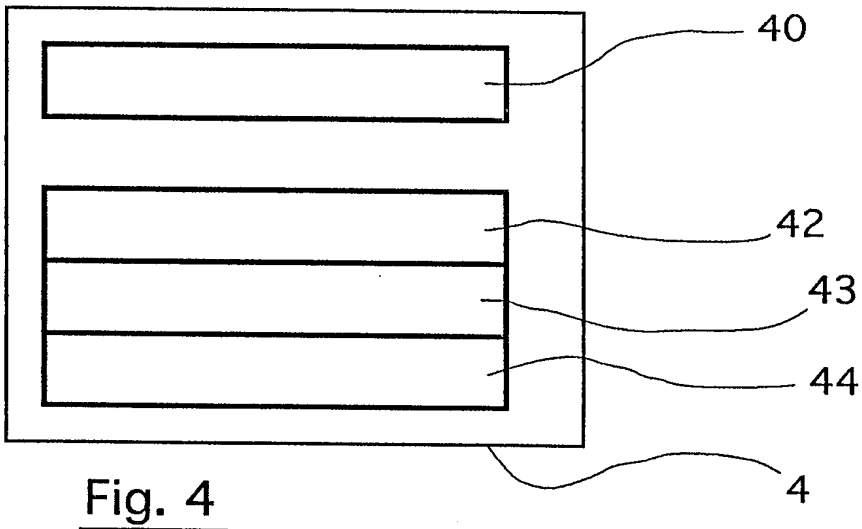

40
42
43
44
4

Fig. 4

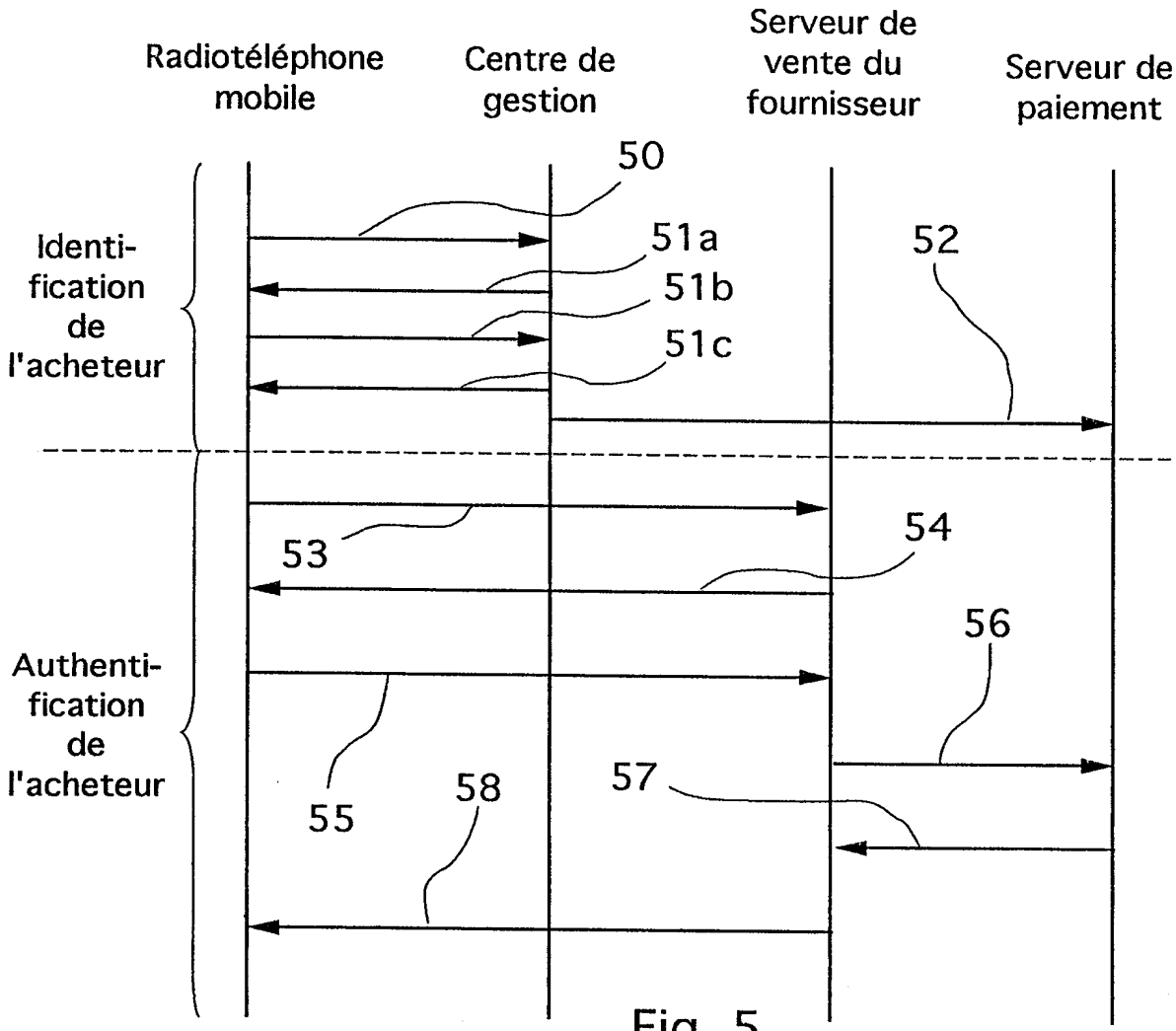

Radiotéléphone mobile
Centre de gestion
Serveur de vente du fournisseur
Serveur de paiement
Identi-fication de l'acheteur
Authenti-fication de l'acheteur
50
51a
51b
51c
52
53
54
55
56
57
58

Fig. 5

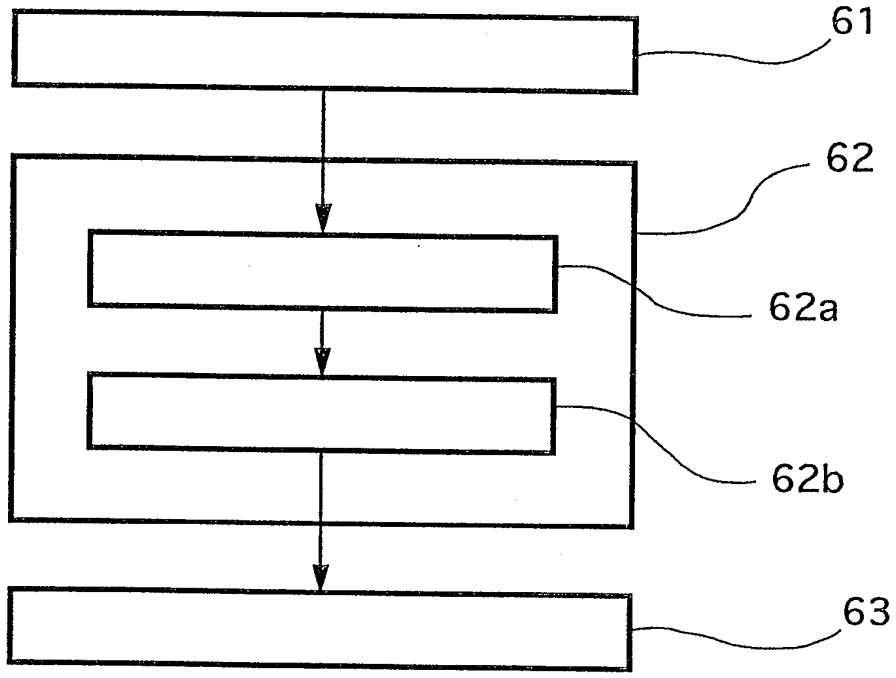


Fig. 6

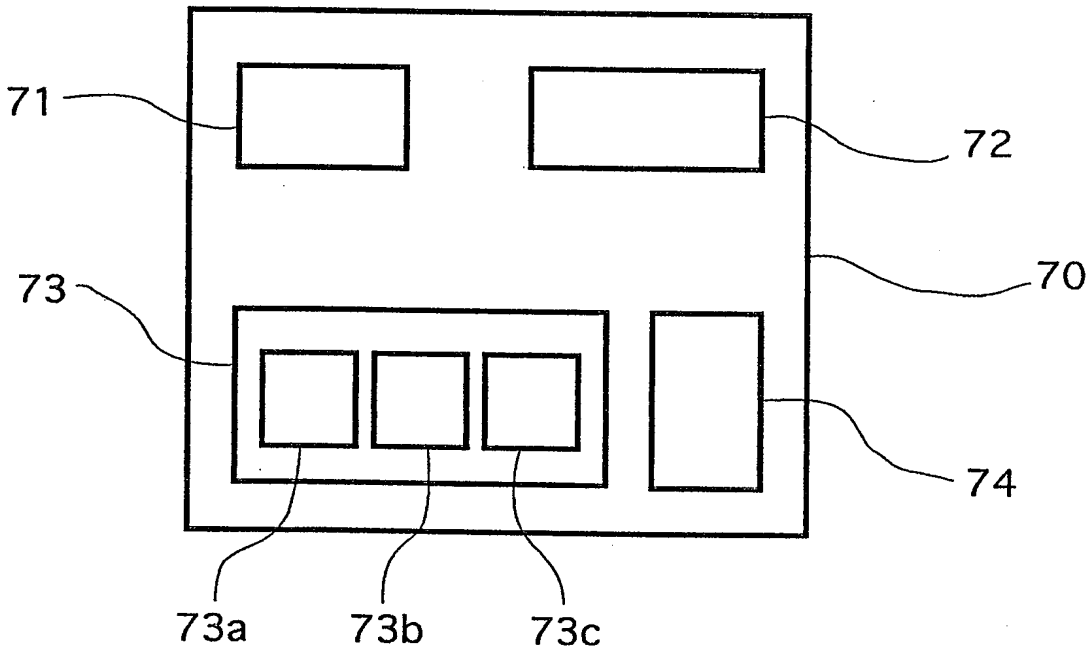


Fig. 7

INTERNATIONAL SEARCH REPORT

Inter ·ional Application No
PCT/FR 99/01436

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M15/00 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M H04Q G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 708 547 A (AT & T CORP) 24 April 1996 (1996-04-24) column 1, line 31 -column 6, line 41; figures 2-6	1 2-5, 10-12, 16,17, 21,22
A	FR 2 740 291 A (SAGEM) 25 April 1997 (1997-04-25) page 2, line 21 -page 8, line 3; figure 2	1-5,10, 12-15, 21,22

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 October 1999	12/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bocage, S

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/FR 99/01436

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 25828 A (NOKIA MOBILE PHONES LTD ;TERHO MIKKO (FI); HEINONEN PETRI (FI); MA) 22 August 1996 (1996-08-22) page 4, line 28 -page 5, line 20 page 9, line 21 -page 11, line 11 page 13, line 3 -page 14, line 3 page 16, line 12 -page 19, line 28 figures 1,5,6 ---	1,2,4,6, 14,18-22
A	US 5 561 706 A (FENNER PETER R) 1 October 1996 (1996-10-01) abstract; claims 1,2 ---	6,7
A	WO 95 01695 A (MOTOROLA INC) 12 January 1995 (1995-01-12) abstract page 4, line 5 -page 8, line 22; figure 2 ---	14
A	EP 0 780 802 A (AT & T CORP) 25 June 1997 (1997-06-25) -----	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/FR 99/01436

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0708547 A	24-04-1996	US 5608778 A	04-03-1997
		CA 2156206 A	23-03-1996
		JP 8096043 A	12-04-1996
FR 2740291 A	25-04-1997	NONE	
WO 9625828 A	22-08-1996	FI 950685 A	16-08-1996
		AU 696876 B	17-09-1998
		AU 4624796 A	04-09-1996
		AU 709016 B	19-08-1999
		AU 7865698 A	22-10-1998
		AU 7865798 A	15-10-1998
		CN 1174648 A	25-02-1998
		EP 0809916 A	03-12-1997
		JP 11501424 T	02-02-1999
		US 5887266 A	23-03-1999
US 5561706 A	01-10-1996	NONE	
WO 9501695 A	12-01-1995	US 5444764 A	22-08-1995
		AU 671383 B	22-08-1996
		AU 7245794 A	24-01-1995
		CN 1110892 A	25-10-1995
		ES 2111484 A	01-03-1998
		FR 2708402 A	03-02-1995
		GB 2285559 A,B	12-07-1995
		GR 94100303 A	22-05-1996
		IT RM940425 A,B	02-01-1995
		SE 9500723 A	18-04-1995
		ZA 9404791 A	20-02-1995
EP 0780802 A	25-06-1997	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Dem · › Internationale No
PCT/FR 99/01436

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04M15/00 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04M H04Q G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 708 547 A (AT & T CORP) 24 avril 1996 (1996-04-24)	1
A	colonne 1, ligne 31 -colonne 6, ligne 41; figures 2-6	2-5, 10-12, 16,17, 21,22

A	FR 2 740 291 A (SAGEM) 25 avril 1997 (1997-04-25) page 2, ligne 21 -page 8, ligne 3; figure 2	1-5,10, 12-15, 21,22

	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
5 octobre 1999	12/10/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bocage, S

2

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/01436

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	WO 96 25828 A (NOKIA MOBILE PHONES LTD ;TERHO MIKKO (FI); HEINONEN PETRI (FI); MA) 22 août 1996 (1996-08-22) page 4, ligne 28 -page 5, ligne 20 page 9, ligne 21 -page 11, ligne 11 page 13, ligne 3 -page 14, ligne 3 page 16, ligne 12 -page 19, ligne 28 figures 1,5,6 ---	1,2,4,6, 14,18-22
A	US 5 561 706 A (FENNER PETER R) 1 octobre 1996 (1996-10-01) abrégé; revendications 1,2 ---	6,7
A	WO 95 01695 A (MOTOROLA INC) 12 janvier 1995 (1995-01-12) abrégé page 4, ligne 5 -page 8, ligne 22; figure 2 ---	14
A	EP 0 780 802 A (AT & T CORP) 25 juin 1997 (1997-06-25) -----	

2

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs à membres de familles de brevets

Demande Internationale No
PCT/FR 99/01436

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0708547	A	24-04-1996	US	5608778 A	04-03-1997
			CA	2156206 A	23-03-1996
			JP	8096043 A	12-04-1996
FR 2740291	A	25-04-1997	AUCUN		
WO 9625828	A	22-08-1996	FI	950685 A	16-08-1996
			AU	696876 B	17-09-1998
			AU	4624796 A	04-09-1996
			AU	709016 B	19-08-1999
			AU	7865698 A	22-10-1998
			AU	7865798 A	15-10-1998
			CN	1174648 A	25-02-1998
			EP	0809916 A	03-12-1997
			JP	11501424 T	02-02-1999
			US	5887266 A	23-03-1999
US 5561706	A	01-10-1996	AUCUN		
WO 9501695	A	12-01-1995	US	5444764 A	22-08-1995
			AU	671383 B	22-08-1996
			AU	7245794 A	24-01-1995
			CN	1110892 A	25-10-1995
			ES	2111484 A	01-03-1998
			FR	2708402 A	03-02-1995
			GB	2285559 A,B	12-07-1995
			GR	94100303 A	22-05-1996
			IT	RM940425 A,B	02-01-1995
			SE	9500723 A	18-04-1995
			ZA	9404791 A	20-02-1995
EP 0780802	A	25-06-1997	AUCUN		